SIEMS Week #2 Homework

Windows Server Logs:

1.Based on the attack signatures, what mitigations would you recommend to protect each user account? Provide global mitigations that the whole company can use and individual mitigations that are specific to each user.

- I would recommend that multi-factor authentication be utilized and password time to live would need to be implemented. The companies worldwide would all need to adhere to these rules to prevent further account tampering.
- Input validation would need to be applied to the entire company worldwide.

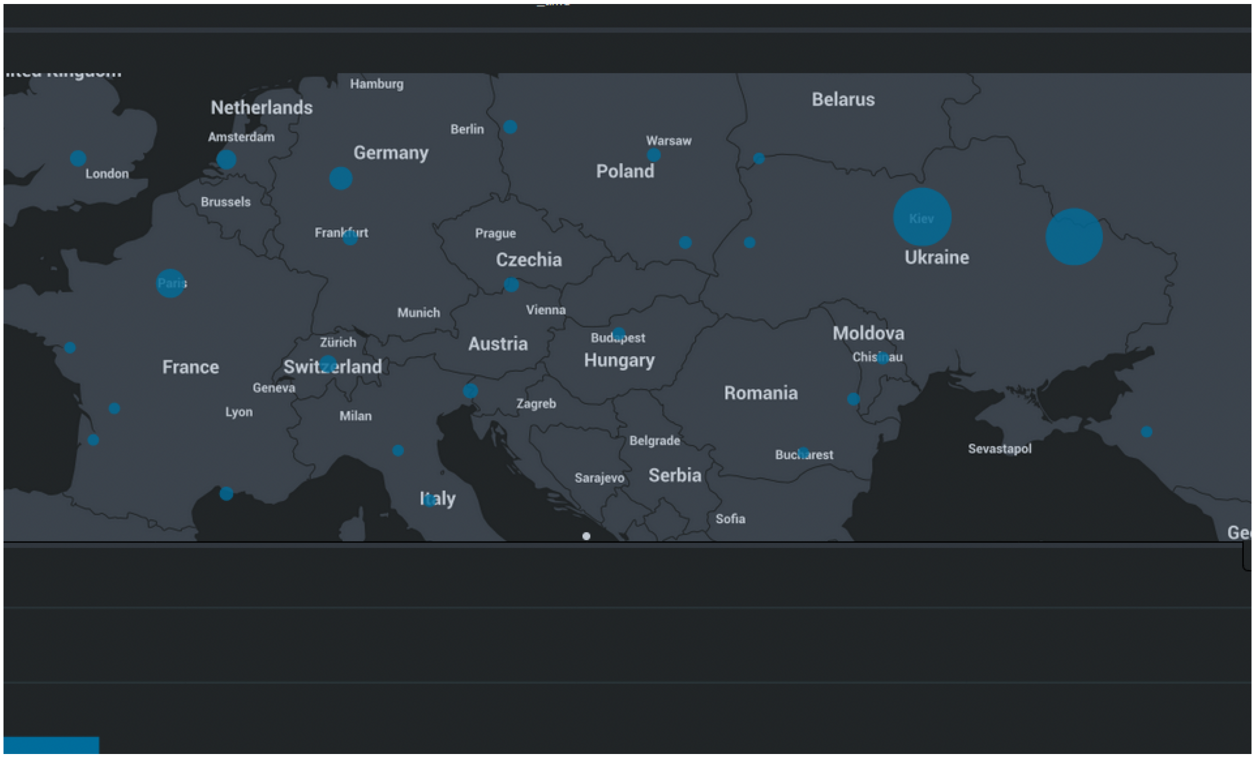
2. VSI has insider information that JobeCorp attempted to target users by sending "Bad Logins" to lock out every user.What sort of mitigation could you use to protect against this?

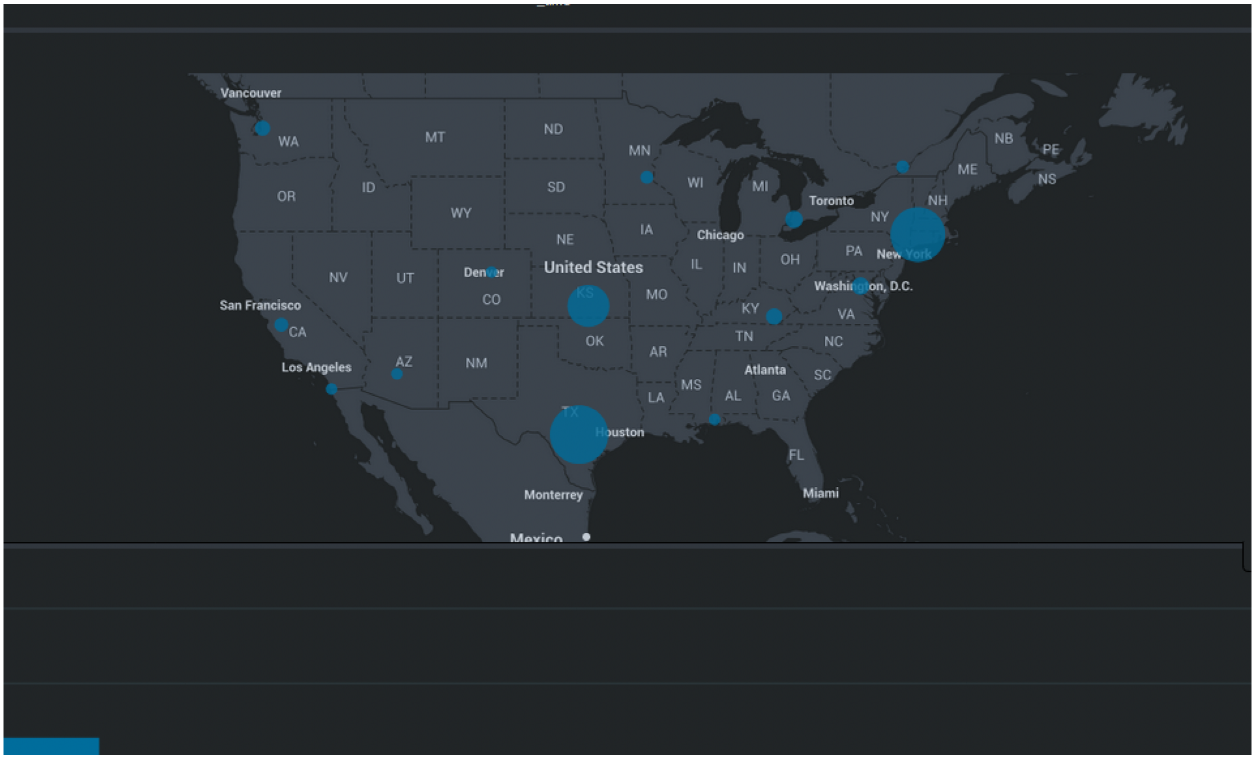
- In order to remedy this attack the company would need to start to use token based authentication keys. This would allow only the employee access to any given workstation.

Apache Server Logs:

1.Based on the geographic map, recommend a firewall rule that the networking team should implement.

- A firewall rule should be implemented blocking all incoming traffic from an unknown source Ip address in the following cities: Kiev, Kharkiv, Hartford, San Antonio, Wichita, and Paris.





2.VSI has insider information that JobeCorp will launch the same webserver attack but use a different IP each time in order to avoid being stopped by the rule you just created.

What other rules can you create to protect VSI from attacks against your webserver?

- Create a firewall rule that specifies that only known source IP addresses (or range of IP addresses), have access to certain services.
- Set a rule that specifies the destination port of the service and block all other port access. The less open ports that are available significantly decreases the likelihood of attack through poor port access configuration.